

GAO

Testimony

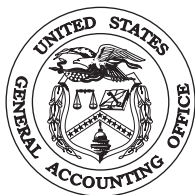
Before the Subcommittee on the District of Columbia,
Committee on Government Reform, House of
Representatives

For Release on Delivery
Expected at
11 a.m.
Friday,
September 24, 1999

YEAR 2000 COMPUTING
CHALLENGE

Status of the District of
Columbia's Efforts to
Renovate Systems and
Develop Contingency and
Continuity Plans

Statement of Jack L. Brock, Jr.
Director, Governmentwide and Defense Information
Systems
Accounting and Information Management Division



GAO

Accountability * Integrity * Reliability

Mr. Chairman and Members of the Subcommittee:

Thank you for inviting me to participate in today's hearing on District of Columbia's Year 2000 (Y2K) challenge. As you know, like most large operations, the District of Columbia is acutely vulnerable to Y2K problems due to its widespread dependence on computer systems for delivering important public services. If these problems are not solved before the end of the year, the District may be unable to effectively carry out its core business operations, such as those to ensure public safety, collect revenue, educate students, and provide health care services. Today, I will discuss the District's progress in fixing its systems and the remaining risks it faces, the actions it needs to take to mitigate these risks over the next 3 months, and the recent experience it needs to capitalize on to strengthen long-term information technology management. In an accompanying statement, we discuss the District's efforts to keep track of the costs associated with addressing the Y2K issue.

Last October, we testified that the District was about 1 year behind recommended Y2K schedules but that positive steps were underway to accelerate its progress in fixing systems.¹ To make the most of the short time remaining, we recommended that the District promptly identify its most important operations, determine which systems supporting these operations could be fixed before the Y2K deadline, and ensure that business continuity and contingency plans are developed for core business operations for which supporting systems cannot be renovated in time. In February 1999, we testified that the District remained far behind schedule, but that its Year 2000 Program Office had taken positive steps to address our earlier recommendations.² We continued to stress, however, that the District's schedule allowed little time for corrective action if needed and vital services remained at risk. As such, we recommended that the District place increased emphasis on completing business continuity and contingency planning efforts and that key stakeholders participate in making critical decisions throughout the remainder of the project.

The District is largely following our recommendations. It has made notable progress in remediating mission-critical systems and has made a good start

¹*Year 2000 Computing Crisis: The District of Columbia Faces Tremendous Challenges in Ensuring Vital Services Are Not Disrupted* (GAO/T-AIMD-99-4, October 2, 1998).

²*Year 2000 Computing Crisis: The District of Columbia Remains Behind Schedule* (GAO/T-AIMD-99-84, February 19, 1999).

in developing business continuity and contingency plans. However, because of its overall late start, the District still faces a very real problem: running out of time. Remediation measures for many mission-critical systems are not yet complete, testing is far from finished, and schedules for some projects have slipped over the last several months. Further, even though the District has made a good start on the initial phase of its business continuity and contingency planning effort, it was not able to give us a complete overview of the status of the next—and most important—phase of its planning work, which will involve adding operational detail and testing of plans. Because so many critical tasks are scheduled for completion over the few remaining months, District management must place increased emphasis on ensuring that project cost and schedule data are accurate, that priorities are established to best focus resources on the remaining system remediation and testing efforts, and that business continuity and contingency planning is completed.

To prepare for this testimony, we conducted an overview of the District's recent efforts to address risks associated with the Y2K date change and compared these efforts to criteria detailed in our *Year 2000 Assessment Guide*,³ *Business Continuity and Contingency Planning Guide*,⁴ and *Testing Guide*.⁵ We reviewed and analyzed a number of key project documents including the District's Enterprise Plan (including updates issued July 27, August 20, August 27, September 3, and September 16, 1999), the District's Quarterly Reports to the Office of Management and Budget (OMB), the District's Emergency Operations Plan, District contingency planning guidance, selected District contingency plans, and Year 2000 Program

³*Year 2000 Computing Crisis: An Assessment Guide* (GAO/AIMD-10.1.14). Published as an exposure draft in February 1997 and finalized in September 1997, the guide was issued to help federal agencies prepare for the Y2K conversion.

⁴*Year 2000 Computing Crisis: Business Continuity and Contingency Planning* (GAO/AIMD-10.1.19). Published as an exposure draft in March 1998 and issued in August 1998, this guide provides a conceptual framework for helping organizations to manage the risk of potential Y2K-induced disruptions to their operations. It discusses the scope and challenge and offers a structured approach for reviewing the adequacy of agency Y2K business continuity and contingency planning efforts.

⁵*Year 2000 Computing Crisis: A Testing Guide* (GAO/AIMD-10.1.21). Published as an exposure draft in June 1998 and issued in November 1998, this guide addresses the need to plan and conduct Y2K tests in a structured and disciplined fashion. The guide describes a step-by-step framework for managing, and a checklist for assessing, all Y2K testing activities, including those activities associated with computer systems or system components (such as embedded processors) that are vendor supported.

Office schedule variance reports. We interviewed District officials responsible for overseeing the Y2K effort, including the Interim City Administrator, the Chief Technology Officer, the Year 2000 Program Manager, the Mayor's Year 2000 Contingency Planning Advisor, the Director of the Emergency Management Agency, the Director for Information Systems Audits in the Office of the Inspector General, and subject matter experts and staff in the Fire and Emergency Medical Services Department. We performed our work in Washington, D.C., from June 11 through September 20, 1999, in accordance with generally accepted government auditing standards.

The District of Columbia Has Further Strengthened Its Y2K Program, But Is Still Behind Schedule

In our earlier testimonies, we emphasized that the District was about 1 year behind recommended schedules; had no margin for taking corrective actions if needed; and, consequently, should complete business continuity and contingency plans as early as possible to allow time for their testing. Since our February testimony, the District has taken actions to strengthen its Y2K project management and continuity and contingency planning. For example, the District has done the following.

- Hired an outside contractor to review its project plan, which tracks baseline and actual milestone dates as well as completion progress, to identify inconsistencies in terms of task sequencing, critical path dependencies, and updating practices.
- Regularly updated its Year 2000 Enterprise Plan and produced a series of variance reports to identify and categorize project milestones extending beyond established date thresholds.
- Hired an outside contractor to oversee the contingency planning effort, establish planning priorities in accordance with current project risks, develop a mechanism for tracking plan implementation and testing in detail, and ensure that the Mayor is provided with accurate, up-to-date information on the contingency planning effort.
- Participated in the Metropolitan Council of Government's Contingency Planning drill held on September 1, 1999, and plans to conduct two drills of its own before January 1, 2000.
- Beginning in June, started to regularly convene its Year 2000 Steering Committee, chaired by Mayor Williams, that brings together top-level decisionmakers from the District's 18 priority agencies, the Control Board, and the City Council.
- Taken steps to establish consistent status reporting across agencies and reconcile differences in data reported by the agencies and the Year 2000

Program Office, which were discovered when preparing the District's most recent Y2K status report for OMB.

While these measures have helped the District to strengthen its ability to oversee the Y2K effort and to better target management attention on high-risk areas, the District has not been able to fully compensate for its late start. This is not surprising given the pervasive nature of the Y2K problem and the complexity involved in fixing systems and ensuring core business processes can continue operating into 2000, especially for a highly decentralized entity such as the District.

System Remediation Status

As of September 20, the District's Chief Technology Officer reported the status of the District's Y2K conversion effort for its mission-critical software applications as follows. Of a total of 223 mission-critical applications, 130 were tested and determined to be ready for the year 2000. Of the remaining 93 mission-critical applications, 70 were reported as currently undergoing testing, and 23 were reported as still being remediated. It should be noted, however, that the status information being reported by the District's Chief Technology Officer is not consistent with information being reported separately by District agencies. For example, in its third quarter Y2K status report to OMB, the District's Year 2000 Program Office, reported that 74 systems are being replaced across the most important, "top 18" agencies, while the agencies report that 35 systems are being replaced. This raises the concern that District managers are not getting accurate enough data on system status on which to base their Y2K-related decisions. District officials told us that they are in the process of reconciling these data differences.

Status of Mission-Critical Projects in the District's Top 18 Agencies

Given the short time left before the Y2K deadline and the extent of the work remaining, the District is now concentrating its efforts on 56 mission-critical projects across its top 18 agencies (which include, for example, the Metropolitan Police Department, Fire and Emergency Medical Services Department, Emergency Management Agency, and Water and Sewer Authority, among other important agencies). The projects can include specific software applications, software infrastructure (e.g., computer operating systems, system utilities, and databases), and "porting"⁶ software

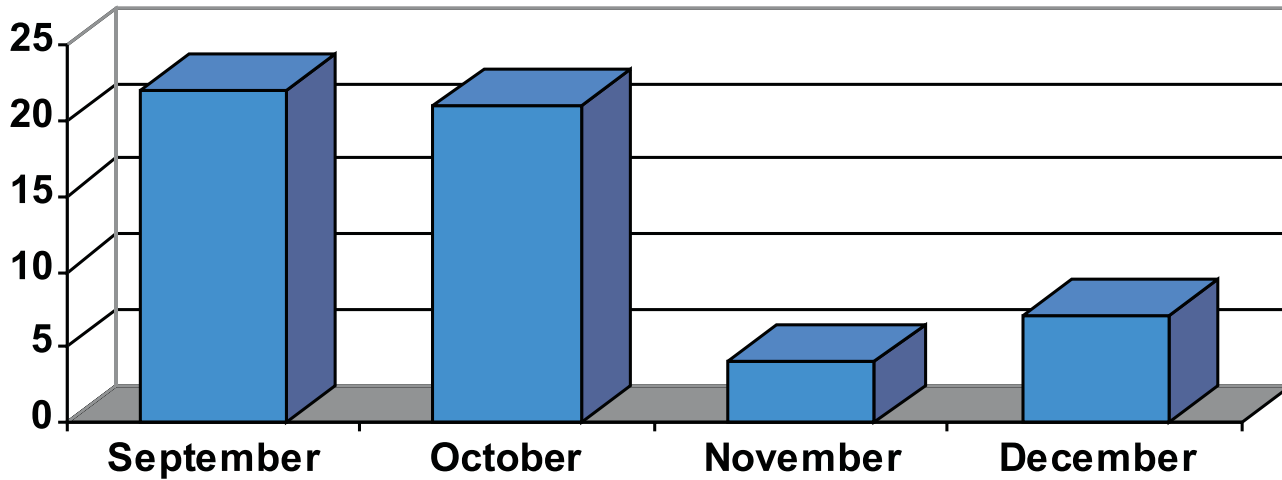
⁶Translating software to run on a different computer and/or operating system.

to Y2K-compliant hardware. According to the District's Year 2000 Enterprise Plan, which was last updated September 16, 1999, a number of the 56 ongoing projects are not scheduled to be tested or implemented until November and December 1999.

- *Testing:* As of September 16, the Year 2000 Enterprise Plan shows that four projects will not be tested until November and another seven in December. As shown in figure 1, this presumes that there will be no schedule slippage on the bulk of testing that is planned for this month and next month. While the District has no other option, completing this effort so close to the Y2K deadline is risky since the testing phase is extremely complex and time-consuming. Y2K conversions often involve numerous large systems with extensive supporting technology infrastructures. As such, before testing can even begin, organizations must develop test plans, define and secure test resources, establish the test environment, develop guidance, and ensure that vendor-supported products and services are Y2K compliant. Once this is done, tests need to be conducted in an incremental fashion, starting first at the software unit level and moving through software integration and system acceptance. When feasible, organizations should also conduct end-to-end tests on their core business processes to ensure that the systems that collectively support the processes can still effectively interoperate.

Figure 1: Testing Schedule as of September 16, 1999

Number of projects

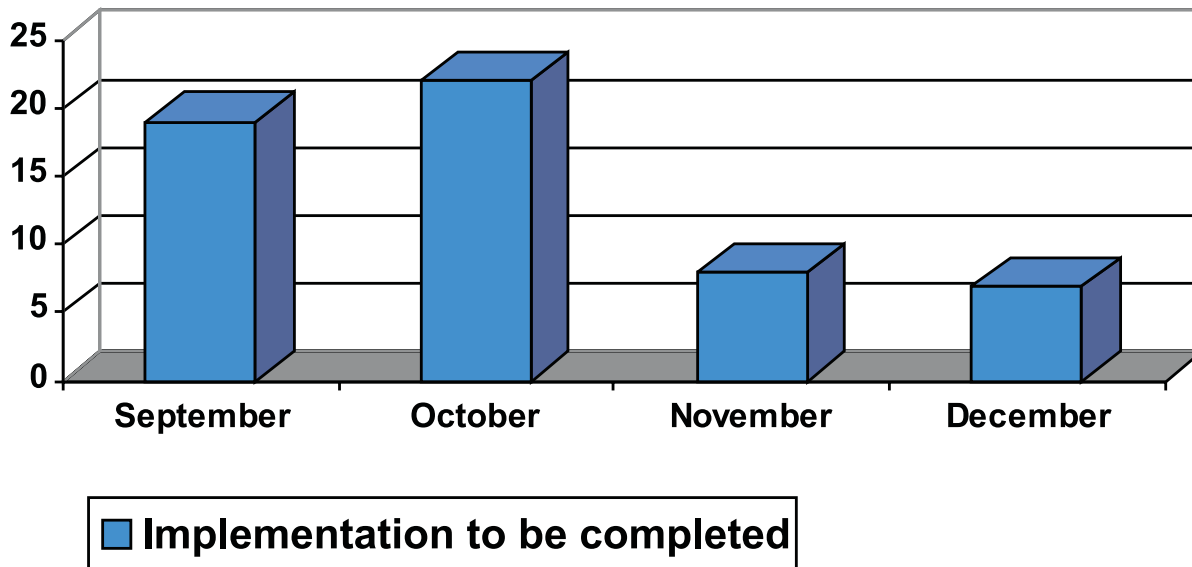


■ Testing to be completed

- *Implementation:* Similarly, the District plans to finish the implementation of eight projects during November and another seven in December. Figure 2 illustrates the District's schedule for completing its implementation work.

Figure 2: Implementation Schedule as of September 16, 1999

Number of projects

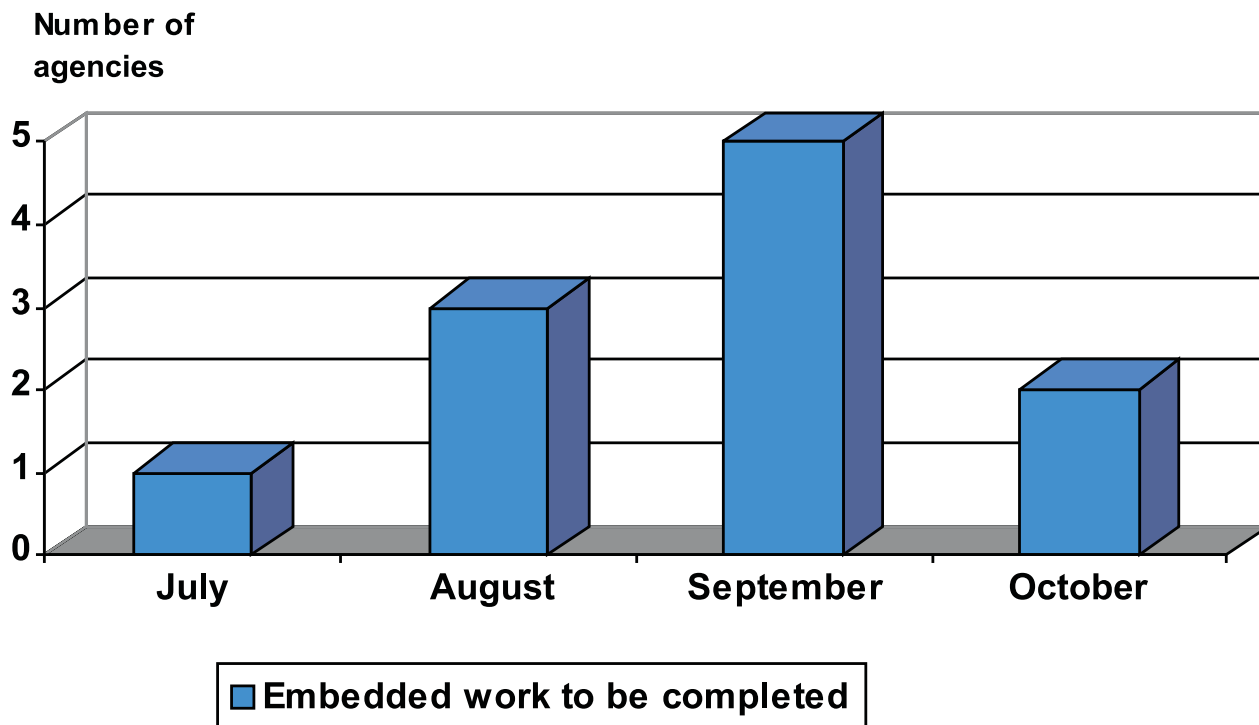


Additionally, the District's schedules are showing some slippage, further compounding its risk. Based on our analysis of the Year2000 Enterprise Plan updates, we found that—since the end of July—29 projects have implementation milestones that have slipped an average of about 2 months.

Embedded Processor Conversion Schedule

The District reports that it is faring somewhat better in fixing its equipment and infrastructure devices with embedded processors that are also vulnerable to Y2K problems (for example, elevators, medical equipment, and alarm systems). Seven of the District's top 18 agencies are reported to be 100 percent complete, 9 are reported to be between 91 and 99 percent complete, 1 is shown as 72 percent complete, and 1 is reported as 66 percent complete. Figure 3 illustrates the District's schedule for completing its embedded work.

Figure 3: Schedule for Completing Embedded Systems/Equipment as of September 16, 1999



Business Continuity and Contingency Planning Schedule

Recognizing the risk associated with its Y2K schedule, the District has implemented a well-defined business continuity and contingency planning effort for its core business processes that is divided into three phases:

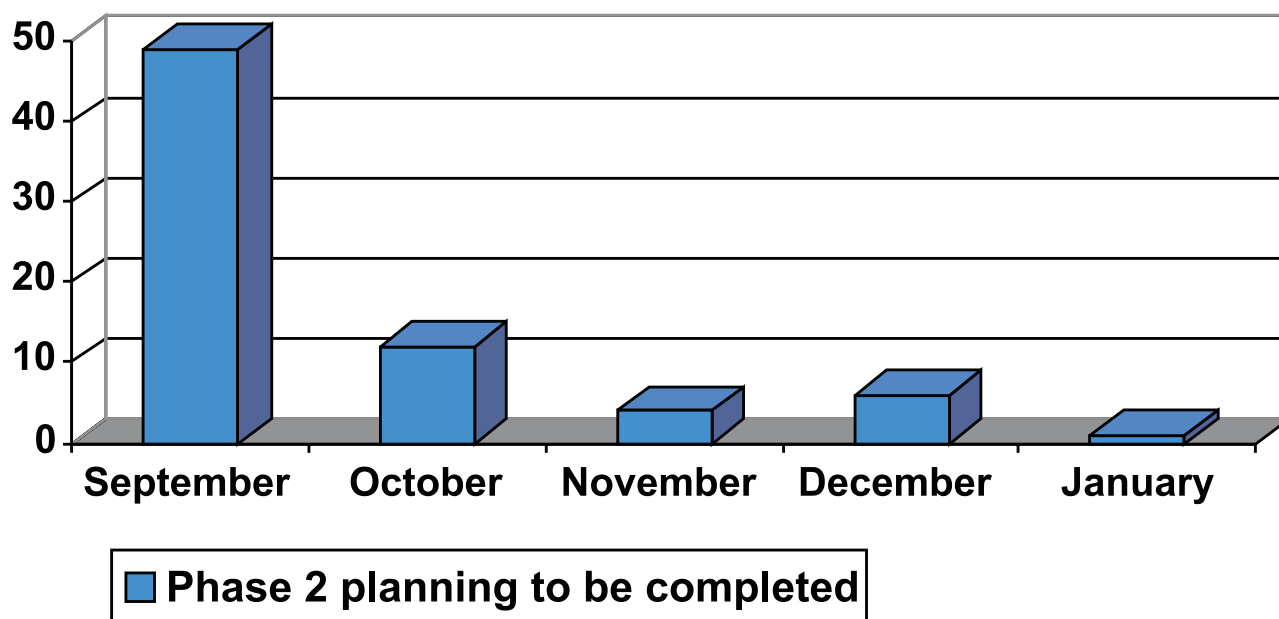
- **Phase 1** is focused on defining a high-level business continuity strategy for each core business process, providing a sense of response to key asset failures.
- **Phase 2** is focused on adding the detail to the plans needed for their testing, refinement, and execution. For example, continuity planning teams will document workaround procedures, describe business process interrelationships, and define resource requirements.
- **Phase 3** is focused on executing the plans and returning to normal operations.

These efforts, too, are running late. The District's September 16 Enterprise Plan for its top 18 agencies shows that although Phase 1 is largely complete, 11 Department of Consumer and Regulatory Affairs

Phase 1 plans are not finished. As shown in figure 4, Phase 2 contingency planning is not expected to be done until close to the century change on January 2000.

Figure 4: Phase2 Contingency Planning Schedule as of September 3, 1999

Number of plans



District contingency planning officials did not have current data on whether Phase 2 planning milestones were being met. They told us that they are working with the heads of the top 18 agencies, the Interim City Administrator, Chief Financial Officer, Chief Technology Officer, and the Chief Procurement Officer to assess the exact status and costs of ongoing continuity and contingency planning efforts and to determine priorities.

Contingency planning officials advised us that the status of this effort would be monitored in accordance with the 5 key planning activities described in the District's Phase 2 planning methodology:

- assessing Phase 1 contingency plans for feasibility,
- ensuring that Phase 1 plans are executable,
- training staff to execute the contingency plans,

-
- testing the contingency plans, and
 - testing plans for returning to normal operations.
-

Steps the District Must Take to Mitigate Risks in the Remaining Months

At this point in time, the District can do little to increase the rate of progress on system remediation and testing. However, the District can improve its chances for success by better using the tools it has at hand. By more aggressively monitoring the status of key projects and ensuring that its status information is accurate, District management can be better-equipped to focus attention on projects running late and redirect resources, if necessary, to ensure that the most critical processes are remediated and tested on time.

Also, viable business continuity plans are important to all organizations—even those that have already completed remediation and testing. They are especially critical to the District because of the real possibility that remediation and testing may not be complete by year's end.

Mr. Chairman, this concludes my testimony on the District's Y2K status. However, I would like to briefly discuss the District's opportunities for using its efforts over the past year as a springboard for improving city services in the future. While the immediate focus for the District over the next 98 days should be on assessing potential risks and business impacts and on prioritizing its remaining efforts, in the long term, the District, like many other organizations confronting the Y2K problem, has a unique opportunity to build on the experience it has gained in putting together its Y2K effort.

The simple reason that the District is so far behind in addressing the Y2K problem is that it did not have effective management over its information technology assets and projects. The District had no management process in place that provided adequate attention to the pending Y2K problem. As a result, it started very late and will finish late. Further, the project team was hampered by a lack of a comprehensive system inventory and limited documentation on key business processes and the systems that supported those processes. Our past reviews of key District systems have also

identified problems in establishing clear project requirements, risk management, security, and software acquisition.⁷

By capitalizing on recent Y2K-related experience, the District can implement management processes and controls needed to ensure that its technology assets are effectively supporting city operations. For example:

- The District has learned that Y2K efforts cannot succeed without the involvement of top-level managers at the agency level and citywide level. Best practices have shown that top executives need to be similarly engaged in periodic assessments of major information technology investments to prioritize projects and make sound funding decisions.⁸ Such involvement is also critical to breaking down cultural and organizational impediments.
- The District has recognized that having complete and accurate information on information systems can facilitate remediation, testing, and validation efforts. Maintaining reliable, up-to-date system information, including a system inventory, is also fundamental to well-managed information technology programs since it can provide senior managers with timely and accurate information on system costs, schedule, and performance.
- The District has developed a better understanding of its core business processes and made some progress in prioritizing its mission-critical systems based on their impact on these processes and the relative importance of the processes themselves. Once the Y2K program is completed, the District can build on these efforts to ensure that information technology initiatives will optimize business processes as well as to identify and retire duplicative or unproductive systems.
- Like many organizations, the District found that special measures were needed to build the technical expertise required to assist with all phases of the Y2K correction process. The same solutions should be pursued for the long term to enhance overall information technology management.

⁷*District of Columbia: Weaknesses in Personnel Records and Public Schools' Management Information and Controls* (GAO/T-AIMD-95-170, June 14, 1995) and *District of Columbia: Software Acquisition Processes for a New Financial Management System* (GAO/AIMD-98-88, April 30, 1998).

⁸*Executive Guide: Improving Mission Performance Through Strategic Information Management and Technology* (GAO/AIMD-94-115, May 1994) and *Assessing Risks and Returns: A Guide for Evaluating Federal Agencies' IT Investment Decision-making* (GAO/AIMD-10.1.13, February 1997).

Mr. Chairman, this concludes my statement. I will be happy to answer any questions you or Members of the Subcommittee may have.

Contact and Acknowledgement

For further information regarding this testimony, please contact Jack L. Brock, Jr. at (202) 512-6240 or by email at brockj.aimd@gao.gov.

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are \$2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary, VISA and MasterCard credit cards are accepted, also.

Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

**U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013**

or visit:

**Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC**

**Orders may also be placed by calling (202) 512-6000
or by using fax number (202) 512-6061, or TDD (202) 512-2537.**

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send an e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web Home Page at:

<http://www.gao.gov>

**United States
General Accounting Office
Washington, D.C. 20548-0001**

**Official Business
Penalty for Private Use \$300**

Address Correction Requested

<p>Bulk Mail Postage & Fees Paid GAO Permit No. GI00</p>
